FILED ON: 9/25/2025

SENATE . . . . . No. 2619

Senate, September 25, 2025 -- Text of the Senate Bill establishing the Massachusetts data privacy act (being the text of Senate document 2608, printed as amended)

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act establishing the Massachusetts data privacy act.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws are hereby amended by inserting after chapter 93L the following chapter:-

Chapter 93M. Massachusetts Data Privacy Act

Section 1. As used in this chapter, the following words shall have the following meanings unless the context otherwise requires:

"Affiliate", a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity; provided, however, that "control" and "controlled" shall mean the: (i) ownership of, or the power to vote, more than 50 per cent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) power to exercise controlling influence over the management of a company.

"Affirmative consent", a clear affirmative act, signifying a consumer's freely given, specific, informed and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a controller; provided, however, that "affirmative consent" shall include a written statement, including by electronic means, or any other unambiguous affirmative action; and provided further, that "affirmative consent" shall not include: (i) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (ii) hovering over, muting, pausing or closing a given piece of content; or (iii) agreement obtained through the use of dark patterns or deceptive design.

"Authenticate", to use reasonable means to determine that a request to exercise any of the rights afforded under this chapter is being made by, or on behalf of, the consumer who is entitled to exercise such rights with respect to the personal data at issue.

"Biometric data", data generated by automatic measurements of a consumer's biological characteristics, such as a fingerprint, a voiceprint or vocal biomarker, eye retinas, irises, gait or personally identifying physical movement or patterns, or other unique biological patterns or characteristics that allow or confirm the unique identification of the consumer; provided, however, that "biometric data" shall not include: (i) a digital or physical photograph; (ii) an audio or video recording; or (iii) any data generated from a digital or physical photograph or an audio or video recording, unless such data is generated to identify a specific individual.

"Business associate", as defined in the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191.

"Child", as defined in the Children's Online Privacy Protection Act, 15 USC 6501.

"Collect", buying, renting, gathering, obtaining, receiving, accessing or otherwise acquiring personal data by any means.

"Consumer", an individual who is a resident of the commonwealth; provided, however, that "consumer" shall not include an individual acting as an employee, an owner, a director, an officer or a contractor of a company, a partnership, a sole proprietorship, a nonprofit organization or a governmental unit whose communications or transactions with a controller occur only within the context of the individual's role with such company, partnership, sole proprietorship, nonprofit organization or governmental unit.

"Controller", a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data.

"Covered entity", as defined in the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191.

"Dark pattern or deceptive design", a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, which shall include, but not be limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

"Decisions that produce legal or similarly significant effects concerning the consumer", decisions that result in access to, or the provision or denial by the controller of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

"De-identified data", data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data: (i) takes reasonable physical, administrative and technical measures to ensure that such data cannot be associated with an individual or be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual; and (ii) contractually obligates any recipients of such data to meet the obligations of clause (i).

"Gender-affirming health care services", as defined in section 11I1/2 of chapter 12.

"Gender-affirming health data", any personal data concerning any effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

"Genetic information", any data, regardless of its format, that concerns a consumer's genetic characteristics, including, but not limited to: (i) raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid of a consumer; or (ii) genotypic and phenotypic information that results from analyzing raw sequence data described in clause (i).

"Identified or identifiable individual", a consumer who can be readily identified, directly or indirectly.

"Legally-protected health care activity", as defined in section 11I1/2 of chapter 12.

"Legally-protected health care data", any personal data concerning any effort made by a consumer to seek, or a consumer's receipt of, legally-protected health care activity.

"Minor", a consumer who has not attained 18 years of age.

"Neural data", any information that is generated by measuring the activity of a consumer's central or peripheral nervous system.

"Person", an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

"Personal data", any information that is linked or reasonably linkable to an identified or identifiable consumer; provided, however, that "personal data" shall not include de-identified data or publicly available information.

"Precise geolocation data", information derived from technology or a device, including, but not limited to, latitude and longitude coordinates from global positioning system mechanisms or other similar positional data, that reveals the past or present physical location of a individual or device that identifies or is linked or reasonably linkable to 1 or more individuals with precision and accuracy within a radius of not more than 1,750 feet; provided, however, that "precise geolocation data" shall not include the content of communications, a photograph or video, metadata associated with a photograph or video that cannot be linked to a individual.

"Process", any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the use, storage, disclosure, analysis, deletion or modification of personal data.

"Processor", a person who collects, processes or transfers personal data on behalf of, and at the direction of, a controller or another processor or a federal, state, tribal or local government entity.

"Profiling", any form of processing performed on personal data to evaluate, analyze or predict personal aspects including a consumer's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

"Protected health information", as defined in 45 CFR 160.103.

"Publicly available information", information that: (i) is lawfully made available through federal, state or municipal government records or widely distributed media; or (ii) a controller has reasonable basis to believe a consumer has lawfully made available to the general public; provided, however, that "publicly available information" shall not include biometric data.

"Reproductive or sexual health care", any supplies, care and services of a medical, behavioral health, mental health, surgical, psychiatric, therapeutic, diagnostic, preventative, rehabilitative or supportive nature relating to pregnancy, contraception, assisted reproduction, miscarriage management, the termination of a pregnancy, a consumer's reproductive system or sexual well-being, including, but not limited to, any such supplies, care and services rendered or provided concerning: (i) a consumer's health condition, status, disease, diagnosis, diagnostic test or treatment; (ii) a social, psychological, behavioral or medical intervention; (iii) a surgery or procedure, including, but not limited to, an abortion; (iv) use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion; (v) a bodily function, vital sign or symptom; (vi) a measurement of a bodily function, vital sign or symptom; or (vii) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

"Reproductive or sexual health data", personal data concerning any effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

"Sale of personal data", the transfer of personal data in exchange for monetary or other valuable consideration by the controller to a third party; provided, however, that "sale of personal data" shall not include: (i) the disclosure of personal data to a processor that processes the personal data on behalf of the controller if limited to the purposes of the processing; (ii) the disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer; (iii) the disclosure or transfer of personal data to an affiliate of the controller; (iv) the disclosure of personal data with the consumer's affirmative consent, where the consumer affirmatively directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; (v) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets; or (vi) the disclosure of personal data that the consumer: (A) intentionally made available to the general public via a channel of mass media; and (B) did not restrict to a specific audience.

"Sensitive data", personal data that includes: (i) a government-issued identifier, including, but not limited to, a social security number, passport number, state identification card or driver's license number; provided, however, that "sensitive data" shall not include a government-issued identifier required by law to be displayed in public; (ii) any personal information that describes or reveals a consumer's mental or physical health condition, diagnosis, disability or treatment, including, but not limited to, gender-affirming health data, reproductive or sexual health data, legally-protected health care data and neural data; (iii) biometric data or genetic information or information derived therefrom; (iv) precise geolocation information; (v) account or device log-in credentials or security or access codes for an account or

device; (vi) personal data of a consumer who a controller or processor knows or should have known is a child; (vii) a consumer's race, color, ethnicity, religion, national origin, citizenship or immigration status; (viii) information revealing a consumer's sex life, sexual orientation or status as transgender or non-binary; or (ix) information that reveals the status of a consumer as a victim of a crime.

"Targeted advertising", displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated internet web sites or online applications to predict such consumer's preferences or interests; provided, however, that "targeted advertising" shall not include: (i) advertisements based on activities within a controller's own web sites or online applications; (ii) advertisements based on the context of a consumer's current search query, visit to a web site or online application; (iii) advertisements directed to a consumer in response to the consumer's request for information or feedback; or (iv) processing personal data solely to measure or report advertising frequency, performance or reach.

"Third party", a person other than the consumer to whom the data pertains or a controller or processor, or affiliate of the controller or processor of the relevant personal data.

"Transfer", disclose, release, disseminate, make available, license, rent or share personal data to a third party orally, in writing, electronically or by any other means.

Section 2. This chapter shall apply to persons that during the preceding calendar year: (i) collected or processed the personal data of not less than 60,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; (ii) collected or processed the personal data of not less than 20,000 consumers and derived not less

than 20 per cent of its gross revenue from the sale of personal data; or (iii) collected, processed or transferred reproductive or sexual health data of consumers. This chapter shall also apply to an affiliate of a person described under this section if such affiliate transferred sensitive data to the person or the person's other affiliates in the preceding calendar year.

Section 3. (a) Notwithstanding section 2, this chapter shall not apply to: (i) a federal, state, tribal, territorial or local government entity, including, but not limited to, a body, authority, board, bureau, commission, district or agency of the commonwealth or of any political subdivision of the commonwealth; (ii) a nonprofit organization established to detect and prevent fraudulent acts in connection with insurance; (iii) a national securities association registered pursuant to section 15A of the Securities Exchange Act of 1934 and the rules and implementing regulations promulgated thereunder; (iv) a registered futures association designated pursuant to section 17 of the Commodity Exchange Act and the rules and implementing regulations promulgated thereunder; (v) a bank, credit union or any affiliate or subsidiary thereof that: (A) is only and directly engaged in financial activities as described in 12 USC 1843(k); (B) is regulated and examined by the division of banks or an applicable federal bank regulatory agency; and (C) has established a program to comply with all applicable requirements established by the commissioner of banks or the applicable federal bank regulatory agency concerning personal data; (vi) an agent, broker-dealer, investment adviser or investment adviser representative, as defined in section 401 of chapter 110A, who is regulated by the secretary of the commonwealth or the United States Securities and Exchange Commission; and (vii) a covered entity or a covered entity's business associate that collected or processed the personal data of not more than 60,000 consumers. Notwithstanding this subsection, a controller or processor who would otherwise be subject to this chapter under section 2 shall not sell sensitive data.

(b) The following information and data shall be exempt from the provisions of this chapter if said information and data are processed, collected or transferred, as applicable, in compliance with relevant federal statutes or regulations, as applicable:

(i) protected health information that a covered entity or business associate collects or processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, and the rules and implementing regulations promulgated thereunder;

(ii) patient-identifying information for purposes of 42 USC 290dd-2;

(iii) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46;

(iv) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(v) identifiable private information collected or processed for the protection of human subjects under 21 CFR Parts 50 and 56 or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with this clause and clauses (iii) and (iv), or other research conducted in accordance with applicable law;

(vi) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.;

(vii) patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, 42 USC 299b-21 et seq.;

(viii) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191;

(ix) personal data regulated by Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.;

(x) personal data regulated by the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq.;

(xi) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq.;

(xii) any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living collected, processed or transferred by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq.; and

(xiii) data collected, processed or transferred: (A) in the course of a consumer applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data are collected and used within the context of that role; (B) as the emergency contact information of a consumer under this chapter used for emergency contact

purposes; or (C) that are necessary to retain to administer benefits for another individual relating to the consumer who is the subject of the information under clause (i) and used for the purposes of administering such benefits.

(c) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, 15 USC 6501 shall be deemed compliant with any obligation to obtain parental consent pursuant to this chapter.

Section 4. (a) A consumer shall have the right to:

(i) confirm whether a controller is collecting or processing the consumer's personal data, including, but not limited to, any inferences about the consumer derived from such personal data, and access such personal data;

(ii) obtain from a controller a list of third parties to which the controller has transferred the consumer's personal data; provided, however, that the attorney general may issue regulations providing for reasonable exemptions or alternatives to this requirement if necessary to protect a controller's trade secrets;

(iii) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(iv) delete personal data provided by, or obtained about, the consumer, including personal data the consumer provided to the controller and personal data the controller obtained from another source;

(v) obtain a copy of the consumer's personal data collected or processed by the controller in a portable and, to the extent technically feasible, readily usable format that allows the

consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

(vi) opt out of the collection and processing of the consumer's personal data for purposes of: (A) targeted advertising; (B) the sale of personal data; or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) (1) If a consumer's personal data is profiled in furtherance of a decision that produces legal or similarly significant effects concerning a consumer, the consumer shall have the right to: (i) question the result of such profiling; (ii) be informed of the reason why the profiling resulted in the decision; (iii) be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future, where feasible; and (iv) review the consumer's personal data used in such profiling.

(2) If the decision is determined to have been based upon inaccurate personal data, the consumer shall have the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

(c) Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise rights pursuant to this subsection.

(1) A controller shall respond to the consumer without undue delay and not more than 45 days after receipt of the request; provided, however, that the controller may extend the response period once by 20 additional days when reasonably necessary, considering the complexity and number of the consumer's requests; provided further, that the controller informs the consumer of any such extension within the initial 45 day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay and not more than 45 days after receipt of the request of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, not less than 2 times per consumer per right during any 12-month period; provided; however, that if requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request; provided further, that the controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under clauses (i) to (v), inclusive, of subsection (a) using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise such right; provided, however, that any such information shall not be used for any purposes other than the authentication of such consumer. A controller shall not require authentication to exercise an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent; provided, however, that if a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made the request disclosing that the controller

believes the request is fraudulent, why the controller believes the request is fraudulent and that the controller will not comply with such request; provided further, that if the request was placed through an agent, both the agent and the person who appointed the agent shall receive that notice.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to clause (iv) of subsection (a) by deleting the consumer's personal data retained by the controller, retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to this chapter.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not more than 60 days after receipt of an appeal, the controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decision. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

(e) A controller shall not condition, effectively condition, attempt to condition or attempt to effectively condition the exercise of a right described in this section through the use of: (i) any false, fictitious, fraudulent or materially misleading statement or representation; or (ii) dark patterns or deceptive design.

(f) A controller shall not collect, process or transfer personal data in a manner that discriminates against, or threaten to discriminate against, an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services, on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, sex, sexual orientation, gender identity, gender expression, disability, religion, genetic information, pregnancy or condition related to pregnancy, status as a veteran, ancestry, national origin, citizenship, immigration status or any other basis protected by chapter 151B.

This subsection shall not apply to: (i) the collection, processing or transfer of personal data for the sole purpose of: (A) a controller self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with federal or state law; or (B) diversifying an applicant, participant or customer pool; or (ii) a private establishment, as described in 42 USC 2000a(e).

(g) (1) A consumer shall be able to exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.

(2) A consumer may designate an authorized agent to exercise the rights specified in clause (vi) of subsection (a). A parent or legal guardian of a child may exercise a consumer right under subsections (a) and (b) on the child's behalf. For a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or conservator of the consumer may exercise a consumer right under said subsections (a) and (b) on the consumer's behalf.

(3) A controller shall comply with a request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

(4) A consumer may designate an authorized agent by technological means, including, but not limited to, an internet link or a browser setting, browser extension or global device setting, that indicates the consumer's intent to opt out of processing for at least 1 of the purposes specified in clause (vi) of subsection (a).

Section 5. (a) A controller shall:

(i) limit the collection of personal data to what is reasonably necessary to provide or maintain a specific product or service requested by the consumer to whom the data pertains;

(ii) unless the controller obtains the consumer's affirmative consent, not process personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer;

(iii) not collect, process or transfer sensitive data concerning a consumer except when such collection, processing or transfer is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;

(iv) not sell sensitive data;

(v) not transfer sensitive data concerning a consumer without obtaining the consumer's affirmative consent or, in the case of the collection or processing of personal data concerning a known child, without collecting or processing such data in accordance with Children's Online Privacy Protection Act, 15 USC 6501 et seq.;

(vi) not collect or process the personal data of a consumer for purposes of targeted advertising or sell the consumer's personal data under circumstances where a controller knows or should have known that the consumer is a minor;

(vii) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue;

(viii) provide an effective mechanism for a consumer that does not use dark patterns or deceptive design to revoke the consumer's affirmative consent that is at least as easy as the mechanism by which the consumer provided affirmative consent and, upon revocation of such affirmative consent, cease to process the data as soon as practicable, but not later than 30 days after the receipt of such request, and shall immediately prevent the transfer of any sensitive data;

(ix) not discriminate or retaliate against, or threaten to discriminate or retaliate against, a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer; and

(x) not sell the precise geolocation data of any individual collected within the commonwealth, regardless of the residency of the individual.

(b) Nothing in clause (ix) of subsection (a) shall be construed to: (i) require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain; or (ii) prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide

loyalty, rewards, premium features, discounts or club card program; provided, however, that the controller shall not transfer personal data to a third party as part of such program unless the transfer of personal data to the third party is clearly disclosed in the terms of the program.

(c) (1) A controller shall provide consumers with a reasonably accessible, understandable, clear, meaningful and not misleading privacy notice that includes:

(i) the categories of personal data collected and processed by the controller, including a separate list of categories of sensitive data collected and processed by the controller, described in a level of detail that provides consumers with a meaningful understanding of the type of personal data collected or processed;

(ii) the purpose for collecting and processing each category of personal data the controller collects or processes described in a way that gives consumers a meaningful understanding of how each category of their personal data will be used;

(iii) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(iv) the categories of personal data that the controller transfers to third parties, if any, and the purposes for those transfers;

(v) the categories of third parties, if any, to which the controller transfers personal data;

(vi) an active electronic mail address or other online mechanism that the consumer may use to contact the controller for privacy and data security inquiries;

(vii) information identifying the controller, including any business name under which the controller registered with the secretary of the commonwealth and any assumed business name that the controller uses in the commonwealth;

(viii) a clear and conspicuous description of any processing of personal data in which the controller engages for the purposes of targeted advertising, sale of personal data to third parties or profiling the consumer in furtherance of decisions that produce legal or similarly significant effects concerning the consumer and a procedure by which the consumer may opt out of this type of processing;

(ix) a general description of the controller's data security practices; and

(x) the effective date of the privacy notice.

(2)(A) The privacy notice shall be: (i) provided directly to consumers in a manner that is reasonably accessible to and usable by individuals with disabilities; and (ii) made available online to the general public.

(B) If a controller makes a material change to its privacy notice, the controller shall notify each consumer affected by the material change prior to implementing the material change with respect to prospectively collected personal data and provide a reasonable opportunity for each consumer to withdraw affirmative consent obtained pursuant to subsection (a). A controller shall provide a reasonable opportunity for each consumer to give affirmative consent to further materially different processing or transfer of previously collected personal data under the changed notice. The controller shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy notice to each affected consumer taking into account available technology and the nature of the relationship.

(d) If a controller sells personal data to a third party or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such sales or processing, as well as the manner in which a consumer may exercise the right to opt out of such sales or processing.

(e) A controller shall establish, and shall describe in a privacy notice, not less than 2 secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights but may require a consumer to use an existing account. The requirements of this subsection are met if the controller:

(i) provides a clear and conspicuous link on the controller's internet website to an internet webpage that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising, the sale of the consumer's personal data and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and

(ii) allows a consumer to opt out of any collection or processing of the consumer's personal data for the purposes of targeted advertising or any sale of the consumer's personal data through an opt-out preference signal sent, with such consumer's affirmative consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale; provided, however, that such platform, technology or mechanism

shall: (A) be consumer-friendly and easy to use by the average consumer; (B) not use dark patterns or deceptive design; (C) require the consumer to provide affirmative consent in order to opt out of any processing of the consumer's personal data; and (D) enable the controller to reasonably determine whether the consumer is a resident of the commonwealth and whether the consumer has made a legitimate request to opt out of any sale of the consumer's personal data or any collection or processing of the consumer's data for targeted advertising; provided further, that for purposes of this subsection, the use of an internet protocol address to estimate the consumer's location shall be considered sufficient to reasonably determine residency.

If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or any sale of personal data through an opt-out preference signal sent in accordance with this subsection conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's financial incentive program or bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with such consumer's opt-out preference signal but may notify the consumer of such conflict and provide to the consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(f) If a controller responds to a consumer opt-out request received pursuant to subsection (e) by informing the consumer of a change in the price, rate, level, quality or selection of goods or services, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) for the processing, sale or transfer of the consumer's personal data.

Section 6. (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Such assistance shall include:

(i) utilizing appropriate technical and organizational measures, as far as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests, taking into account the nature of processing and the information available to the processor;

(ii) assisting the controller in meeting the controller's obligations in relation to the security of processing personal data and in relation to the notification of a breach of security of the system of the processor, taking into account the nature of processing and the information available to the processor; and

(iii) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be in writing, binding and shall include, but not be limited to, clearly set forth instructions for processing data and protecting the confidentiality of the data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties including a method by which the processor shall notify the controller of material changes to its privacy practices. The processor shall adhere to the instructions of the controller and only process and transfer the data it receives from the controller to the extent necessary to provide a service requested by the controller, as set out in the contract. The contract shall also require that the processor:

(i) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(ii) at the controller's direction, delete or return all personal data to the controller as requested, unless retention of the personal data is required by law;

(iii) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

(iv) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the contractual, statutory and regulatory obligations of the processor with respect to personal data;

(v) be prohibited from combining personal data that the processor receives from or on behalf of a controller with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual; and

(vi) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; provided, however, that the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter; provided further, that commonly accepted industry assessment procedures for data protection are utilized for any such assessments; and provided further, that the processor shall provide a report of any such assessment to the controller upon request.

(c) A processor shall establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data that are consistent with chapter 93H and appropriate to the volume and nature of the personal data at issue.

(d) Nothing in the contract required pursuant to subsection (b) shall relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship.

(e) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under this chapter.

(f) A processor shall not process or transfer personal data on behalf of a controller if the processor knows or has reason to believe that the controller has willfully disregarded or violated this chapter with respect to such personal data.

(g) A controller that acquires personal data as part of a merger, acquisition, bankruptcy or other transaction in which the controller assumes control of all or part of another person's assets shall provide affected consumers with notice of such acquisition following the acquisition.

Notice to consumers under this subsection shall include the name of the controller receiving the consumer's personal data, the applicable privacy policies of the controller and notice of the rights available to consumers under section 4. The attorney general may issue rules and promulgate regulations prescribing the form of notice under this subsection and establishing mechanisms to facilitate a consumer's exercise of rights pursuant to clause (iv) of subsection (a) of section 4 or other provisions of this chapter.

Section 7. (a) A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment for each of the controller's processing activities that presents such heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer shall include, but not be limited to, the:

(i) collection or processing of personal data for the purposes of targeted advertising;

(ii) sale of personal data;

(iii) processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of: (A) unfair or deceptive treatment of, or unlawful disparate impact on, a consumer; (B) financial, physical or reputational injury to a consumer; (C) a physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of a consumer, where such intrusion would be offensive to a reasonable person; or (D) other substantial injury to a consumer; and

(iv) collection or processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) shall identify the categories of personal data collected, the purposes for collecting such personal data, whether personal data is being transferred and identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that are employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(d) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall satisfy the requirements established in this section if such data protection assessment is similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(e) (1) A controller shall, upon request of the attorney general, disclose a data protection assessment to the attorney general.

(2) The attorney general may evaluate a data protection assessment for the controller's compliance with the requirements of this chapter. A controller's data protection assessment may be used in an action to enforce this chapter.

(3) To the extent that any information contained in the data protection assessment disclosed to the attorney general includes information subject to the attorney-client privilege or work product protection, the disclosure shall not constitute a waiver of such privilege or protection.

(4) A data protection assessment obtained by the attorney general shall be confidential and shall be exempt from section 10 of chapter 66.

Section 8. (a) Nothing in this chapter shall be construed to: (i) require a controller or processor to re-identify de-identified data; (ii) maintain data in identifiable form or collect, obtain, retain or access any data or technology in order to be capable of associating an authenticated consumer request with personal data; or (iii) require a controller or processor to comply with an authenticated consumer rights request if the controller: (A) is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data; and (B) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer.

(b) A controller that transfers de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Section 9. (a). Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

(i) comply with federal law or other laws of the commonwealth;

(ii) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities, except as prohibited by another law, including, but not limited to, section 115 of chapter 93;

(iii) cooperate with a federal law enforcement agency or any law enforcement agency of the commonwealth concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal or state law;

(iv) investigate, establish, exercise, prepare for or defend legal claims;

(v) provide a product or service specifically requested by the consumer;

(vi) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(vii) take steps at the request of a consumer prior to entering into a contract;

(viii) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and where the processing cannot be manifestly based on another legal basis;

(ix) prevent, detect, protect against, investigate, prosecute those responsible for or otherwise respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any other type of illegal activity;

(x) preserve the integrity or security of systems;

(xi) engage in public or peer-reviewed scientific, historical or statistical research in the public interest that adheres to all relevant laws and regulations governing such research, if

applicable, and is approved, monitored and governed by an institutional review board or similar independent oversight entity that determines whether the: (A) deletion of personal data requested by a consumer under clause (iv) of subsection (a) of section 4 is likely to provide substantial benefits that do not accrue exclusively to the controller; (B) expected benefits of the research outweigh the privacy risks; and (C) controller has implemented reasonable safeguards to mitigate privacy risks associated with the research, including any risks associated with re-identification;

(xii) assist another controller, processor or third party with any of the obligations under this chapter;

(xiii) process personal data for reasons of public interest in the area of public health, community health or population health solely to the extent that such processing is: (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law;

(xiv) ensure the security and integrity of personal data as required by this chapter, protect against spam or protect and maintain networks and systems, including through diagnostics, debugging and repairs;

(xv) effectuate a product recall pursuant to federal or state law or fulfill a warranty;

(xvi) perform internal operations from data collected in accordance with this section that are reasonably aligned with the expectation of the consumer based on the consumer's existing relationship with the controller; and

(xvii) publish entity-based member or employee contact information where such publication is intended to allow members of the public to contact such member or employee in the ordinary course of the entity's operations.

(b) (1) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor would violate an evidentiary privilege.

(2) Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the commonwealth as part of a privileged communication.

(c) Nothing in this chapter shall be construed to:

(i) impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, freedom of speech and freedom of the press guaranteed in the First Amendment to the United States Constitution and Article XVI of the Constitution of the Commonwealth;

(ii) apply to any person's collection or processing of personal data in the course of such person's personal or household activities;

(iii) for private schools approved under section 1 of chapter 76 and private institutions of higher education as defined by 20 USC section 1001 et seq., require deletion of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution;

(iv) prevent access to the data of a child by the child's parent or guardian; or

(v) for a consumer reporting agency, as defined in 15 USC 1681a(f), require deletion of personal data used for the purpose of evaluating a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, subject to the provisions of the Fair Credit Reporting Act, 15 USC 1681 et seq.

(d) (1) Personal data collected or processed by a controller pursuant to this section may be collected or processed to the extent that such collection and processing is: (i) reasonably necessary to effectuate the purposes listed in this section; (ii) limited to what is necessary in relation to the specific purposes listed in this section; and (iii) compliant with subsection (f) of section 4.

(2) Personal data processed pursuant to subsection (a) shall, where applicable, take into account the nature and purpose or purposes of such processing. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such processing of personal data.

(e) If a controller collects or processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such collection or processing qualifies for the exemption and complies with the requirements in this subsection.

Section 10. (a) The attorney general may adopt, amend or rescind rules and regulations for the implementation, administration and enforcement of this chapter.

(b) A violation of this chapter shall constitute an unfair or deceptive trade practice for purposes of chapter 93A. Notwithstanding sections 9 and 11 of said chapter 93A, the attorney

general shall have exclusive authority to bring a civil action against a controller or processor that violates this chapter or a regulation adopted under this chapter to:

(i) enjoin an act or practice that is in violation of this chapter or a regulation adopted under this chapter, including an order that an entity retrieve any personal data transferred in such violation;

(ii) enforce compliance with this chapter or a regulation adopted under this chapter, including seeking declaratory relief;

(iii) obtain damages, including punitive damages, restitution of any money or property obtained directly or indirectly by any such violation, and disgorgement of any profits, assets, property, or data obtained directly or indirectly by any such violation on behalf of the residents of the commonwealth;

(iv) impose civil penalties in an amount not more than $5,000 per violation;

(v) obtain investigative costs, reasonable attorney's fees and other litigation costs, including, but not limited to, expert fees, reasonably incurred; and

(vi) obtain any such other and further relief as the court may deem proper.

(c) The attorney general shall create, maintain and monitor a mechanism for consumers to report potential violations of this chapter.

(d) (1) Prior to initiating any action for a violation of any provision of this chapter, the attorney general shall issue a notice of violation to the controller unless the attorney general determines that a cure is not possible or an alleged violation requires immediate enforcement. If

the controller fails to cure such violation not more than 60 days after receipt of the notice of violation, the attorney general may bring an action pursuant to this section.

(2) In determining whether an alleged violation requires immediate enforcement, the attorney general may consider: (i) the number of violations; (ii) the size and complexity of the controller or processor; (iii) the nature and extent of the controller's or processor's processing activities; (iv) the likelihood of injury to the public; (v) the safety of persons or property; (vi) whether the alleged violation was likely caused by a human or technical error; (vii) whether the alleged violation directly or indirectly resulted in or caused unauthorized data access, theft or disclosure; and (viii) the extent to which the controller or processor has violated this chapter or similar laws in the past.

SECTION 2. Subsection (d) of section 10 of chapter 93M of the General Laws is hereby repealed.

SECTION 3. Section 1 shall take effect on January 1, 2027.

SECTION 4. Section 2 shall take effect on June 1, 2027.